Attorney Docket RSW920020011US1

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

February 14, 2007

In re application of David A. Bruton, et al.

Serial No.: 10/058,689 Filed: January 28, 2002

For: Intrusion Event Filtering and Generic Attack Signatures

Art Unit: 2137 Examiner: Zachary A. Davis

RESPONSE TO NOTICE TO FILE CORRECTED APPLICATION PAPERS

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

sent by fax to 571-270-9803

Attn: Mr. Dale G. Olson, Office of Patent Publication

Sir:

This Response is in reply to the Notice to File Corrected Application Papers (hereinafter, "the Notice") dated February 7, 2007, a copy of which is submitted herewith. The following remarks are respectfully submitted.

The Notice states that a line is crossed out in **FIG. 18**. This is intentional. The crossed-out line (i.e., a line **1870** with an "X" placed thereupon) is discussed on p. 48 of Applicants' specification, lines 1 - 2, which state "The "X" on the arrow extending from probe **1870** to rule **1810** is intended to illustrate that the rule is not applicable for this probe."

Accordingly, Applicants respectfully submit that **FIG. 18** is correct as currently presented, and request that the Notice be withdrawn.

Respectfully submitted,

Marcia L. Doubet

Marcia L. Doubet
Attorney for Applicants
Reg. No. 40,999

Cust. Nbr. for Correspondence: 43168
Phone: 407-343-7586
Fax: 407-343-7587

Attached: Notice to File Corrected Application Papers, including Identification of Drawing Deficiencies (2 pages total)

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Serial No.	:	10/058,689
Applicant	:	Bruton et al.
Filing Date	:	1/28/02
Date Mailed	:	2/7/07

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

This application has been accorded an Allowance Date and is being prepared for issuance. The application, however, is incomplete for the reasons below.

Applicant is given 60 days from the mail date of this Notice within which to correct the informalities indicated below. If the informality pertains to the abstract, specification (including claims) or drawings, the informality must be corrected with an amendment in compliance with 37 CFR 1.121 (or, if the application is a reissue application, 37 CFR 1.173). Such an amendment may be filed after payment of the issue fee if limited to correction of informalities noted herein. See Waiver of 37 CFR1.312 for Documents Required by the Office of Patent Publication, 1280 Off. Gaz. Patent Office 918 (March 23, 2004). In addition, if the informality is not corrected until after payment of the issue fee, for purposes of 35 U.S.C. 154(b)(1)(iv), "all outstanding requirements" will be considered to have been satisfied when the informality has been corrected. A failure to reply will result in the application being ABANDONED. **This period for reply is NOT extendable under 37 CFR 1.136(a).**

See attachment.

A copy of this notice MUST be returned with the reply. Please address response to "Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450".

Dale G. Olson
Office of Patent Publication
Phone: 703-308-9250 ext.122

Application No. 10/058,689 Drawings filed 1-28-02

IDENTIFICATION OF DRAWING DEFICIENCIES

□ There is a hole or the image thereof within the illustration. FIG(s)________

□ The character of the lines, numbers and letters is poor. FIG(s) ________

□ The illustration is penetrated or traversed by a solid or broken line that is not intended to be part of the drawing, such as a dark line caused by a flaw in the copying process. FIG(s)________

□ An ink stamp or an image obscures part of the illustration. FIG(s)________

□ The drawing is marred by black smudges, obliterations, or fax/copier marks. FIG(s)________

□ Figure numbers are duplicated or missing. FIG(s). ________

☒ Numbers, letters, or reference characters in the drawing have been crossed out by hand or are illegibly handwritten. FIG(s) 18 A line is crossed out.

□ The drawing's background shows that the original drawing was made on graph paper or other paper with a pattern or decoration. FIG(s)________

□ The FIG. number label is placed in a location that causes the drawing to be read upside down. FIG(s)________

□ Data, a reference number, or part of the drawing is truncated or missing. FIG(s)________

□ The drawing is continued onto a second page (or more) without proper labeling under 37 CFR 1.81(u)(1). FIG(s)________

□ The drawing and/or the FIG. label contain(s) foreign language. FIG(s)________

□ Color drawings are present in this application but the following CFR 1.84 (a) requirements have not been met*:

- □ Petition filed
- □ Petition fee
- □ 3 sets of color drawings
- □ Color drawing paragraph

*If color drawings are not elected, then applicant must respond so stating. Also, references to color drawings in the specification, if any, must be amended.

COMMENTS:

The "X" on the arrow extending from probe 1870 to rule 1810 is intended to illustrate that the rule is not applicable for this probe.

The final correlation shown in Fig. 18 is between probe 1880 and rule 1820. Probe 1880 presumably sets the ConditionType parameter to "attack" and the AttackType parameter to "fragment", and determines that the current event is of medium suspicion. Because the condition part of rule 1820 is matched in this example and the rule specifies that it applies for the medium sensitivity level, and table 1500 indicates that the event therefore counts, an arrow is shown extending from probe 1880 to rule 1820.

By specifying sensitivity levels in each rule, as shown in Fig. 18, a fine-grained approach to filtering events can be achieved. (Alternatively, a system-wide sensitivity level might be used to provide a coarse-grained filtering; in this case, individual sensitivity levels are not required.)

As illustrated at 1890 in Fig. 18, the sensitivity/suspicion level technique can be applied in an implementation that maps the prior art detailed, attack-specific signatures from a signature file to the IDS policy (i.e. the rules in policy repository 1800) which is described herein. (This approach is beneficial in a network-based IDS solution.) As shown at 1891, a packet having all code bits set may be considered a malformed packet attack which has a high suspicion level (as indicated by the syntax elements "<malformed>" and "<HS>"). The signature at 1892, applying to packets having the SYN or FIN bits set along with a source port number of "0", is also considered a malformed packet attack which has a high suspicion level. Signatures 1893 and 1894